



Vendor: Fortinet

Exam Code: NSE6_SDW_AD-7.6

Exam Name: Fortinet NSE 6 - SD-WAN 7.6 Enterprise
Administrator

Version: DEMO

QUESTION 1

Refer to the exhibit. The event log on a FortiGate device is shown.

Based on the output shown in the exhibit, what can you conclude about the tunnels on this device?

```
6: date=2024-12-18 time=15:15:06 eventtime=1734563705745090691 tz="-0800" logid="0113022925" type="event" subtype="sdwan" level="information" vd="root" logdesc="SDWAN SLA information" eventtype="SLA" healthcheck="HUB1_HC" slatargetid=1 interface="HUB1-VPN3" status="up" latency="1.001" jitter="0.162" packetloss="0.000" moscodec="g711" mosvalue="4.404" inbandwidthavailable="10.00Gbps" outbandwidthavailable="10.00Gbps" bibandwidthavailable="20.00Gbps" inbandwidthused="0kbps" outbandwidthused="0kbps" bandwidthused="0kbps" slamap="0x1" msg="Health Check SLA status."

7: date=2024-12-18 time=15:14:26 eventtime=173456366633265394 tz="-0800" logid="0101037141" type="event" subtype="vpn" level="notice" vd="root" logdesc="IPsec tunnel statistics" msg="IPsec tunnel statistics" action="tunnel-stats" remip=120.64.1.1 locip=192.2.0.1 remport=500 locport=500 outintf="port1" srccountry="Reserved" cookies="50b8a3684ddfd2cb/af3f725d883c5585" user="10.0.64.1.1" group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=172.168.1.1 vpntunnel="VPN4_0" tunnelip=N/A tunnelid=3050027470 tunneltype="ipsec" duration=2968 sentbyte=245849 rcvbyte=246456 nextstat=600 fctuid="N/A" advpnsc=0

8: date=2024-12-18 time=15:04:26 eventtime=1734563066334261977 tz="-0800" logid="0101037141" type="event" subtype="vpn" level="notice" vd="root" logdesc="IPsec tunnel statistics" msg="IPsec tunnel statistics" action="tunnel-stats" remip=100.64.33.1 locip=192.2.0.1 remport=4500 locport=4500 outintf="port1" srccountry="Reserved" cookies="c0f150ded109a548/165f413d17cecc49" user="Branch3" group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=N/A vpntunnel="HUB1-VPN1_0" tunnelip=192.168.1.4 tunnelid=3050027486 tunneltype="ipsec" duration=1122 sentbyte=92064 rcvbyte=0 nextstat=600 fctuid="N/A" advpnsc=1

9: date=2024-12-18 time=15:04:26 eventtime=1734563066334252138 tz="-0800" logid="0101037141" type="event" subtype="vpn" level="notice" vd="root" logdesc="IPsec tunnel statistics" msg="IPsec tunnel statistics" action="tunnel-stats" remip=172.16.1.1 locip=172.16.0.1 remport=500 locport=500 outintf="port4" srccountry="Reserved" cookies="c0c2c62ecc04871/a4d93a059b8df005" user="172.16.1.1" group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=192.168.1.193 vpntunnel="HUB2-VPN3" tunnelip=N/A tunnelid=3050027467 tunneltype="ipsec" duration=2367 sentbyte=195836 rcvbyte=196492 nextstat=600 fctuid="N/A" advpnsc=0
```

- A. The voice traffic is steered through the VPN tunnel HUB1-VPN3.
- B. The VPN tunnel HUB1-VPN1_0 is a shortcut tunnel.
- C. The master tunnel HUB2-VPN3 cannot accept auto-discovery VPN (ADVPN) shortcuts.
- D. There is one shortcut tunnel built from the master tunnel VPN4.

Answer: B

Explanation:

In the IPsec tunnel statistics logs, the field `advpnsc` indicates whether the tunnel is an ADVPN shortcut (`advpnsc=1`) or a regular/master tunnel (`advpnsc=0`). In the output, the entry for `vpntunnel="HUB1-VPN1_0"` shows `advpnsc=1`, while the entries for `VPN4_0` and `HUB2-VPN3` show `advpnsc=0`. Therefore, HUB1-VPN1_0 is an ADVPN shortcut tunnel.

QUESTION 2

You want FortiGate to use SD-WAN rules to steer local-out traffic.

Which two constraints should you consider? (Choose two.)

- A. By default, FortiGate uses SD-WAN rules only for local-out traffic that corresponds to ping and traceroute.
- B. By default, local-out traffic does not use SD-WAN.
- C. You can steer local-out traffic only with SD-WAN rules that use the manual strategy.
- D. You must configure each local-out feature individually to use SD-WAN.

Answer: BD

Explanation:

By default, local-out traffic does not use SD-WAN → FortiGate normally sends local-out traffic (e.g., DNS, NTP, FortiGuard updates) directly through its interfaces without applying SD-WAN rules.

You must configure each local-out feature individually to use SD-WAN → To steer local-out traffic

via SD-WAN, you must explicitly configure the desired local-out features (e.g., DNS, FortiGuard, CAPWAP) to use SD-WAN rules.

QUESTION 3

Refer to the exhibit. What can you conclude from the output shown?

```

London_1 # diagnose sys sdwan service4 3

Service(3): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
Tie break: cfg
Shortcut priority: 3
Gen(33), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(sla), sla-compare-order
Member sub interface(9):
  4: seq_num(4), interface(HUB1-VPN1):
    1: HUB1-VPN1_0(30)
    2: HUB1-VPN1_1(35)
  5: seq_num(5), interface(HUB1-VPN2):
    1: HUB1-VPN2_0(31)
Members(9):
  1: Seq_num(4 HUB1-VPN1_1 HUB1), alive, sla(0x1), gid(0), cfg_order(0), local cost(0), selected
  2: Seq_num(4 HUB1-VPN1_0 HUB1), alive, sla(0x1), gid(0), cfg_order(0), local cost(0), selected
  3: Seq_num(5 HUB1-VPN2_0 HUB1), alive, sla(0x1), gid(0), cfg_order(1), local cost(0), selected
  4: Seq_num(4 HUB1-VPN1 HUB1), alive, sla(0x1), gid(0), cfg_order(0), local cost(0), selected
  5: Seq_num(5 HUB1-VPN2 HUB1), alive, sla(0x1), gid(0), cfg_order(1), local cost(0), selected
  6: Seq_num(6 HUB1-VPN3 HUB1), alive, sla(0x1), gid(0), cfg_order(2), local cost(0), selected
  7: Seq_num(7 HUB2-VPN1 HUB2), alive, sla(0x2), gid(0), cfg_order(3), local cost(10), selected
  8: Seq_num(8 HUB2-VPN2 HUB2), alive, sla(0x2), gid(0), cfg_order(4), local cost(10), selected
  9: Seq_num(9 HUB2-VPN3 HUB2), alive, sla(0x2), gid(0), cfg_order(5), local cost(10), selected
Src address(2):
  10.0.0.0-10.255.255.255
  10.0.1.0-10.0.1.255
Dst address(2):
  10.0.1.0-10.0.1.255
  10.0.0.0-10.255.255.255
    
```

- A. It is a spoke device. SD-WAN rule 4 allows three shortcuts tunnels.
- B. It's a hub device. It allowed the establishment of three auto-discovery VPN (ADVPN) shortcuts.
- C. It is a spoke device. SD-WAN rule 3 is configured with nine members.
- D. It is a spoke device. The members of SD-WAN rule 3 are grouped into two zones.

Answer: C

Explanation:

The command output is from `diagnose sys sdwan service4 3`, which shows details for Service(3) on a spoke (London_1). Under "Members(9)" you can see nine SD-WAN members listed (HUB1-VPN1/HUB1-VPN2 with their shortcut subinterfaces, plus HUB2 VPN members). Therefore, this spoke's SD-WAN rule 3 is configured with nine members.

QUESTION 4

Your FortiGate is in production. To optimize WAN link use and improve redundancy, you enable and configure SD-WAN.

What must you do as part of this configuration update process?

- A. Replace references to interfaces used as SD-WAN members in the routing configuration.
- B. Purchase and install the SD-WAN license, and reboot the FortiGate device.
- C. Replace references to interfaces used as SD-WAN members in the firewall policies.
- D. Disable the interface that you want to use as an SD-WAN member.

Answer: C

Explanation:

When you enable SD-WAN on a FortiGate, the individual WAN interfaces that you add into the SD-WAN zone are no longer referenced directly in firewall policies.

Instead, you must update those firewall policies to use the SD-WAN zone as the interface reference.

QUESTION 5

Refer to the exhibit. The administrator configured the IPsec tunnel VPN1 on a FortiGate device with the parameters shown in exhibit.

Based on the configuration, which three conclusions can you draw about the characteristics and requirements of the VPN tunnel? (Choose three.)

```
config vpn ipsec phase1-interface
  edit "VPN1"
    set interface "port1"
    set ike-version 2
    set peertype any
    set exchange-interface-ip enable
    set mode-cfg disable
    set proposal aes256-sha256
    ...
  end
end
```

- A. The tunnel interface IP address on the spoke side is provided by the hub.
- B. The remote end can be a third-party IPsec device.
- C. The administrator must manually assign the tunnel interface IP address on the hub side
- D. The remote end must support IKEv2.
- E. This configuration allows user-defined overlay IP addresses.

Answer: CDE

Explanation:

The administrator must manually assign the tunnel interface IP address on the hub side

The setting "set exchange-interface-ip enable" means the tunnel interface IP address is exchanged, but the hub side IP must be set manually.

The remote end must support IKEv2

The command "set ike-version 2" explicitly configures IKE version 2 for this tunnel, so the remote device must support IKEv2.

This configuration allows user-defined overlay IP addresses

The tunnel interface enables user control over IP addressing for the overlay network, allowing custom IP assignments.

QUESTION 6

Refer to the exhibits. The administrator configured a device blueprint and CLI scripts as shown in

the exhibits, to prepare for onboarding FortiGate devices in the company's stores. Later, a technician prepares a FortiGate 51G with a basic configuration and connects it to the network. The basic configuration contains the port1 configuration and the minimal configuration required to allow the device to connect to FortiManager.

After the device first connects to FortiManager, FortiManager updates the device configuration.

Based on the exhibits, which actions does FortiManager perform?

Device blueprint

Edit Device Blueprint - Stores ✕

Name	Stores
Device Model	FortiGate-51G ▼
Automatically Link to Real Device	☒
Enforce Firmware Version	☐
Enforce Device Configuration i	☒
Add to Device Group	☐
Add to Folder	☐
Fabric Authorization Template	☐
Pre-Run CLI Template	☒ 5G-links ▼
Assign Policy Package	☒ default ✕ ▼
Provisioning Templates	corp_st ✕ LAN-interface ✕ +
HA	☐

CLI script LAN-interface

Edit CLI Template – LAN interface

Name

LAN-interface

Type

CLI

Comments

Script details

Search...

↑
↓

```

1 config system interface
2     edit port1
3         set mode dhcp
4         set allowances ping https ssh fgfm
5     next
6     edit port2
7         set mode dhcp
8     next
9     edit port5
10        set ip 10.0.${branch_id}.254 255.255.255.0
11        set allowaccess ping
12    end
13 end

```

- FortiManager updates the device configuration according to the selected templates. It applies the corp_st template first.
- FortiManager does not update the port1 configuration because FortiManager does not change the configuration of interfaces with fgfm access.
- FortiManager updates access rights only for port1. FortiManager cannot update the IP address because it was already set manually.
- FortiManager updates the configuration of port1, port2, and port5. The three ports might get new IP addresses.

Answer: D

Explanation:

Enforce Device Configuration is enabled and the blueprint applies the provisioning CLI templates. The LAN-interface script sets port1 and port2 to DHCP and assigns a static IP to port5 (using the branch_id variable). Therefore, when FortiManager pushes the blueprint, it updates the configurations of port1, port2, and port5 - and their IP addresses may change accordingly.

QUESTION 7

Refer to the exhibit. You configure SD-WAN on a standalone FortiGate device. You want to create an SD-WAN rule that steers Facebook and LinkedIn traffic through the less costly internet link. The FortiGate GUI page appears as shown in the exhibit.

What should you do to set Facebook and LinkedIn as destinations?

Settings

Info

Name

Social_app

Status

↑ Enabled

↓ Disabled

Source

Address

4 LAN-net

×

+

User group

+

Destination

Address

+

Internet service

+

Outgoing Interfaces

Interface selection strategy

● Manual

Manually assign outgoing members.

- A. Install a license to allow applications as destinations of SD-WAN rules.
- B. In the **Internet service** field, select **Facebook** and **LinkedIn**.
- C. Enable the applications as destinations of the SD-WAN rule feature visibility.
- D. You cannot configure applications as destinations of an SD-WAN rule on a standalone FortiGate device.

Answer: B

Explanation:

In an SD-WAN rule, you can steer application traffic by using Internet Service Database (ISDB) entries. Facebook and LinkedIn are predefined ISDB objects in FortiGate, so the correct way is to select them in the Internet service field under Destination. This ensures that all traffic to these applications is matched and routed through the chosen (less costly) link.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.lead2pass.com/all-products.html>



Microsoft



ORACLE



JUNIPER
NETWORKS



EMC²
where information lives

10% Discount Coupon Code: ASTR14